Privacy Protection in the Generative AI Era

Christopher Parsons
Senior Technology & Policy Advisor

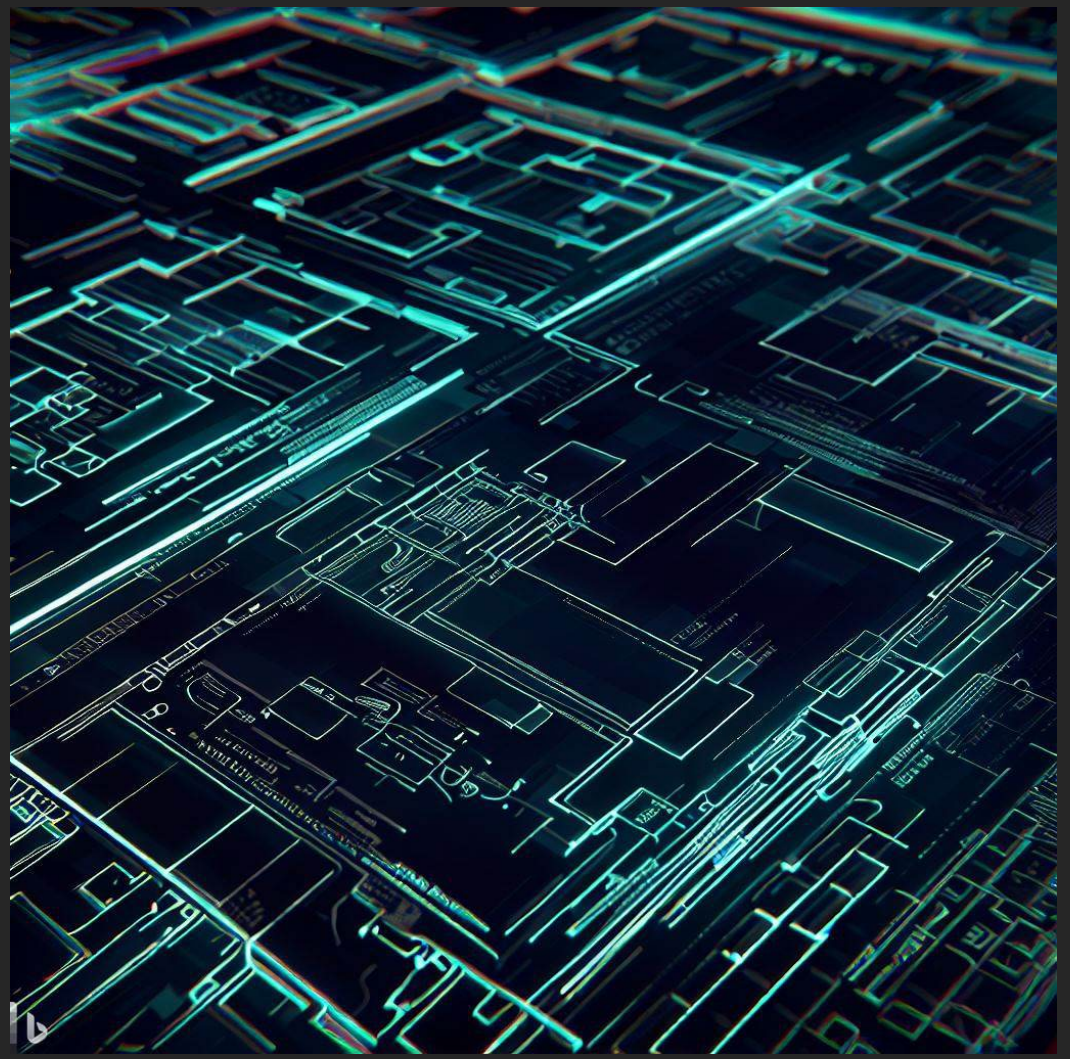
Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

IAPP Webinar

June 8, 2023

Structure

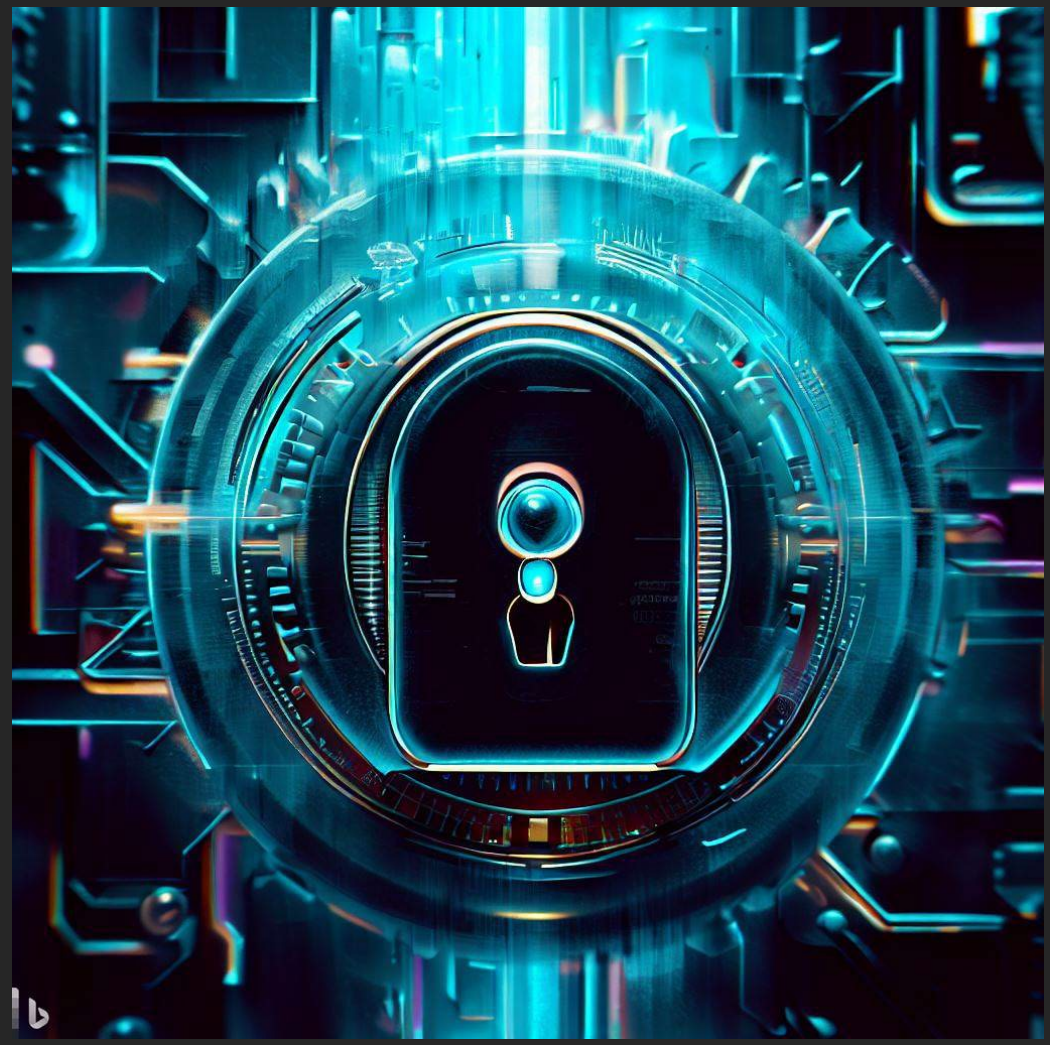
1. Background to IPC
2. International Developments
3. National Turn and AIDA
4. Ontario's Guidance
5. Limitations and Challenges
6. IPC Undertakings
7. Potential Policy Instruments



<Caveat>

The Information and Privacy Commissioner

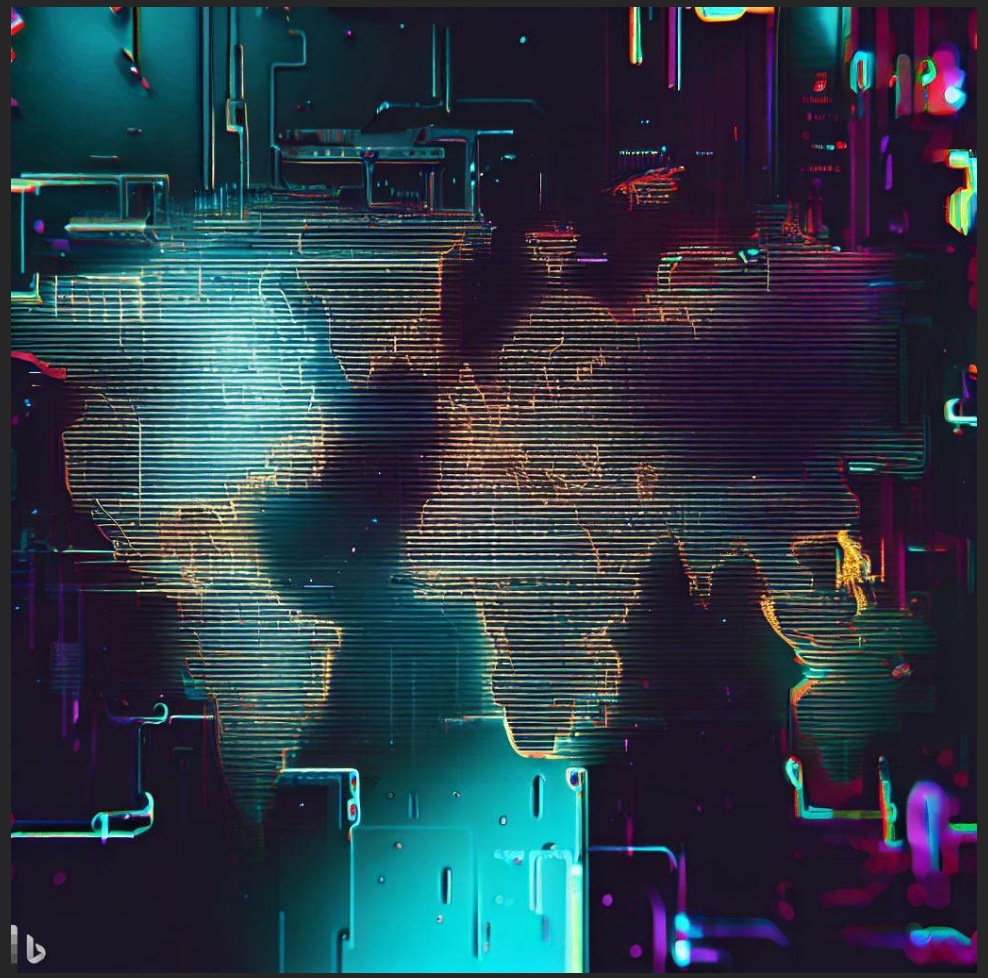
- Commissioner Kosseim (2020)
- Public organizations
- Division of IPC
- Strategic priorities
- Amongst other elements of mandate:
  - Conduct research and provide comment
  - Educate Ontarians on privacy laws and current issues



International Action

International

- G7: Hiroshima Communique
- USA: NIST, White House, FTC
- EU: AI Act
- Europeans: French, Spanish, and UK AI Regulators
- China: Generative AI Regulation



The National Turn: AIDA

- Part of C-27 and at INDU
- Apply to “high-impact” systems
- Focused on cross-provincial trade and commerce
- 2+ years to pass regulation
- Regulators could use existing powers
- Industry Minister oversees and enforces

Ontario's AI Governance

- 2021 Trustworthy AI Consultation
- Draft AI guidance
  - Transparency Guidelines
  - Principles for Ethical Use

Transparency Guidelines (Alpha)

1) Identify data-enhanced decisions
2) Keep people in focus and in the loop
3) Provide public notice and clear communications channels
4) Assess expectations and outcomes
5) Allow meaningful access
6) Describe related data
7) Support rules, requirements, and reporting
8) Update regularly

Principles for Ethical Use (Beta)

1) Transparency and explainable
2) Good and fair
3) Safe
4) Accountable and responsible
5) Human centric
6) Sensible and appropriate

Bias, Equity, and Discrimination

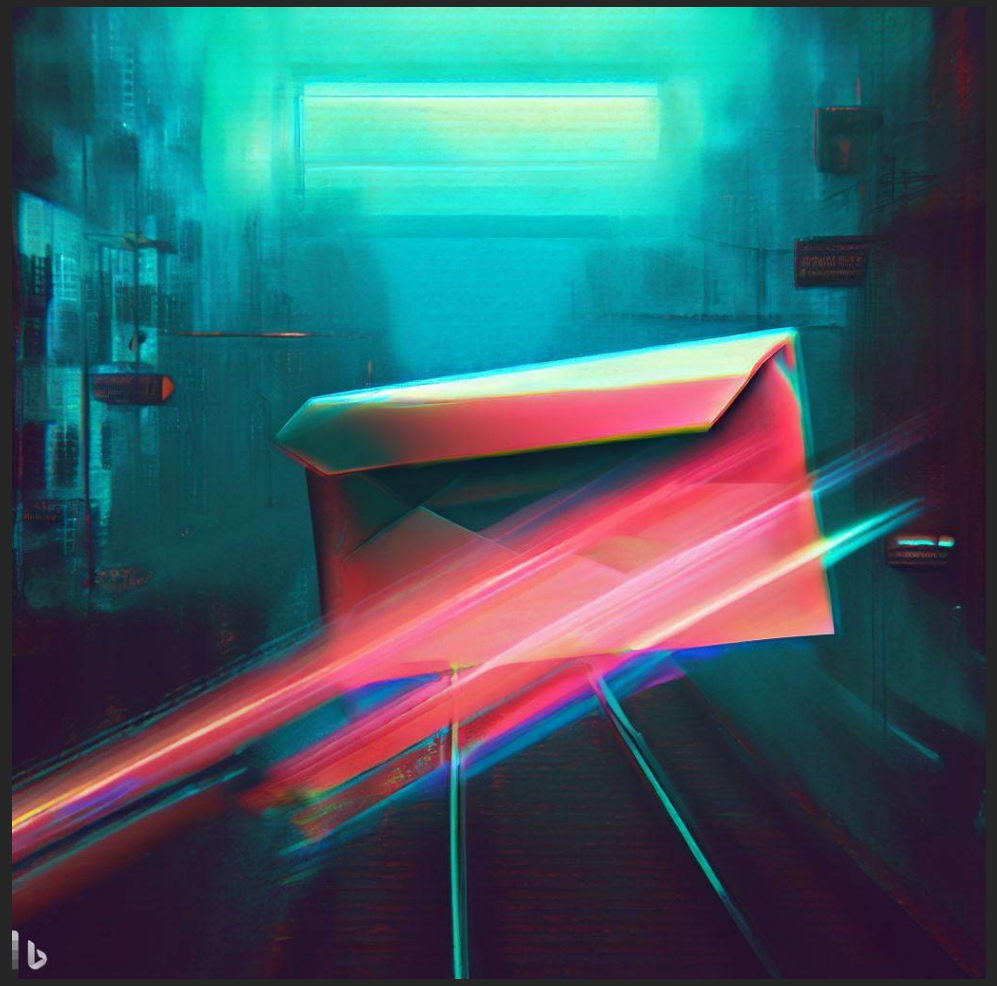
- AI systems have historically exhibited bias
- Fairness questions pervade their deployment for medium- and high-risk systems
- Discrimination is often challenging to detect
- In Machines We Trust

Pressing Challenges

1. Training Data: De-biased? Sourced legally?
2. Large Language Model Memories: Emits intimate images?
3. Model Update Costs: Expensive to fix
4. Variable Outputs: Inconsistent generative responses
5. Class Breaks: Break once, break everywhere
6. Attack Surfaces: Experts unsure how to secure

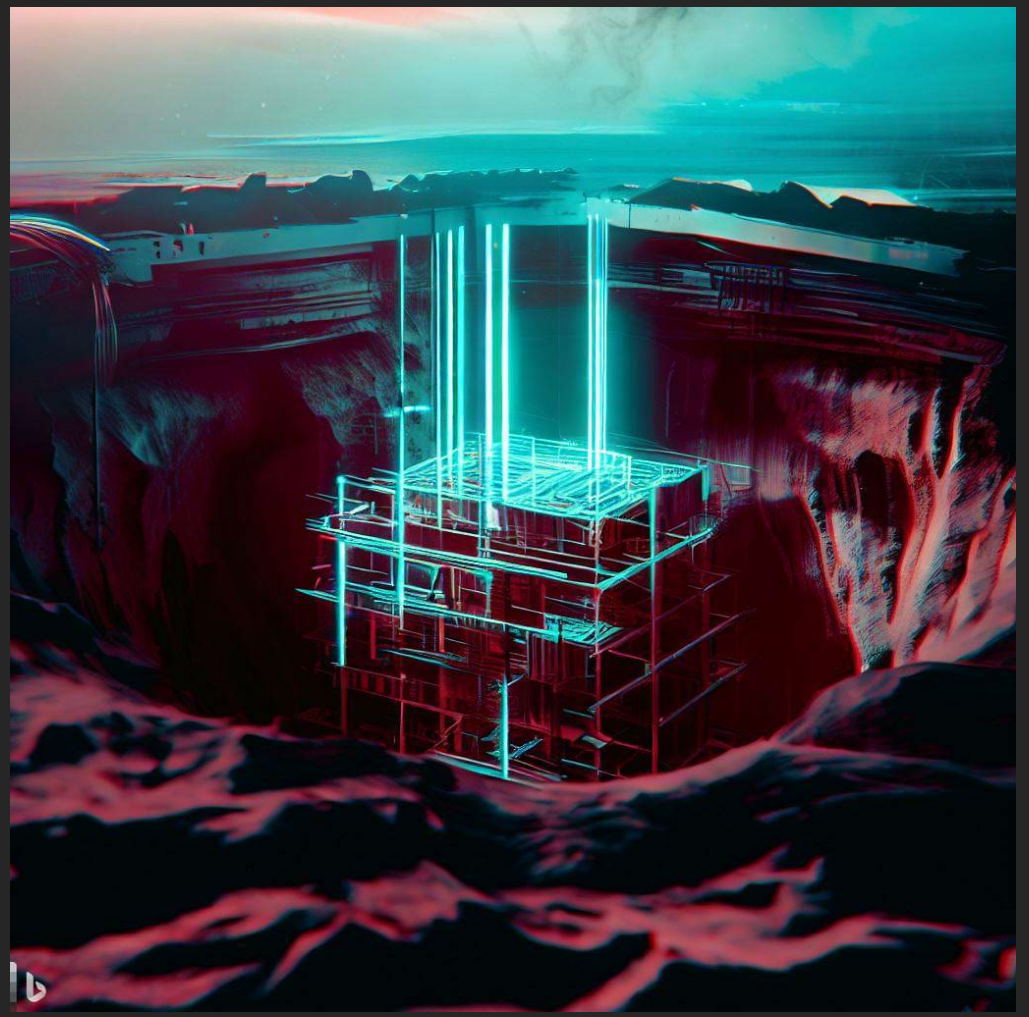
IPC and OHRC Joint Statement

- Calling for stronger guardrails
  - Safety
  - Privacy
  - Accountability
  - Transparency (and access rights)
  - Human Rights
- Origins of personal information
- Limitations of de-identification
- Importance of meaningful consultation



Considerations For A Future Ontario Policy Instrument

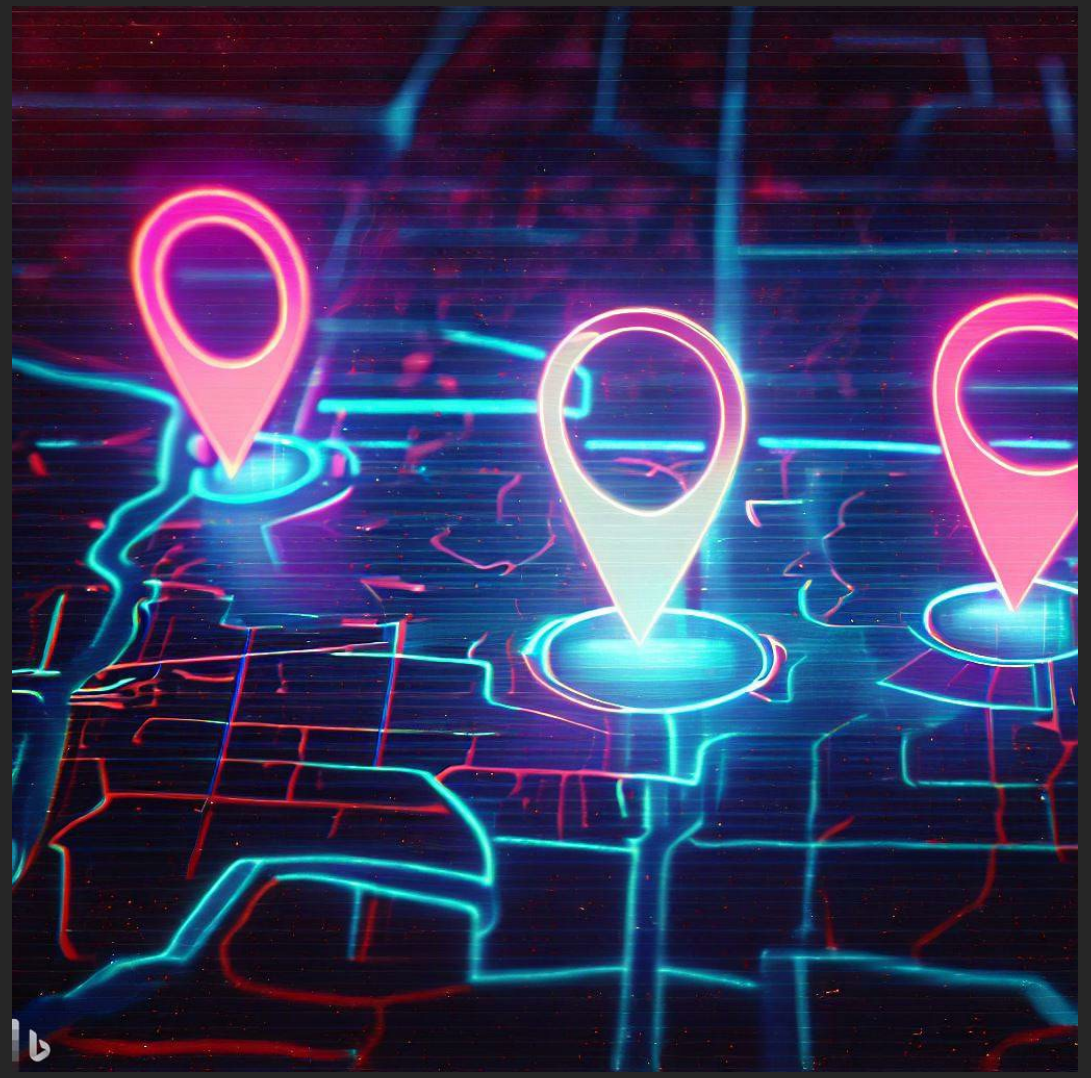
- Clarity
- Assessment and Transparency
- Operational
- Consultation



What Kind of Instrument?

- Framework?
- Ministerial Directive?
- Legislation and Regulation?

- IPC currently lacks a strong position on the specific instrument



Contact Me

- E: Christopher.Parsons@ipc.on.ca